Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Monday, August 20, 2007

Smart contracts watch

Cell phones can be used to monitor and pay for parking. This system and this one are pretty clumsy in terms of all the gratuitous user input required, but as has occurred with prepaid cell phones I expect this to become quite a bit more user-friendly in the future. It will be very nice to be able to top up the parking meter without having to return to the car.

As usual remember that any information recorded (here, where and when you park) "can and will be used against you." For example it can generally be subpoenad for use in court, as also occurs with credit card records, phone records, and automated toll systems. My old boss David Chaum, his student Stefan Brands, and others in the advanced cryptography community have designed many protocols that would preserve privacy in these scenarios, but the deployers of these technologies are usually not terribly interested in your privacy. Your recourse -- keep using physical cash, and take the trouble to go back to your car to check and stuff your parking meter.

In my original writing on smart contracts I talked about trading derivatives and constructing synthetic assets with low transaction costs:

> Very complex term structures for payments (ie, what payments get made when, the rate of interest, etc.) can now be built into standardized contracts and traded with low transaction costs, due to computerized analysis of these complex term structures. Synthetic assets allow us to arbitrage the different term structures desired by different customers, and they allow us to construct contracts that mimic other contracts, minus certain liabilities. As an example of the latter, synthetic assets have been constructed that mimic the returns of stocks in German companies, without requiring payment of the tax foreigners must pay to the German government for capital gains in German stocks.

A bit later I figured out that the primary barrier to such activity is mental transaction costs. These costs throw a monkey wrench into what is otherwise the very good idea of consumer derivatives. One can imagine a wide variety of consumer derivatives, such as buying insurance against air fare changes and the growing business of selling sports tickets based on personal seat licenses (PSLs). I have sketched some possible solutions to the mental transaction problem, such as the market translator. The main problem is designing an automated agent that can figure out user preferences without bothering the user -- usually by recording and analyzing the user's normal behavior. If this can be fully automated the bottom drops out, so to speak, and even nanobarter becomes possible.

Smart contracts, based on digital property, open up a vast new space of possibilities. Many of the digital machines you own can obtain good information about your usage and their own status, from which they could at least crudely estimate what you want to buy. Take parking, for example. A suitably smart car and parking meter system should be able to figure out where you want to park and how much you want to pay for it, with minimal user intervention. I'm not talking anything like "AI" here, just computerized cars and parking

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

meters that have sufficient sensors, can communicate with each other, and use known algorithms. As you are driving down the street, you tell your car that you want to find a parking place. The price of open parking spots ahead starts popping up on your dashboard. You choose and agree to pay the fee by simply parking in the spot.

Along with this future urban lifesaver, parking spot derivatives would be very useful. For the same reasons as stadium owners sell PSLs -- to receive revenue up-front to help pay the cost of building the infrastructure -- owners of parking spaces could sell parking space licenses (PSL again, oops :-). The owner of the PSL, in turn -- or said owner's car acting as his agent -- could sell the hours or minutes that the car is not using. You could buy a PSL and thereby reserve that sweet spot right next to your downtown office for the year. Then sell off the parking rights for the weekends. You could reserve a spot next the your favorite club and sell off all the times except Thursday through Saturday night. And if you are away from the office or staying in for the evening, your car's market translator can price and offer the space and it will become open and start popping up on driver's dashboards.

This kind of thing is just the tip of the iceberg as far as the potential of smart contracts is concerned.

Finally I will report on a digital cash system from no less than our frequent commentor Daniel Nagy. Nagy makes the following observation:

> While everyone with a cellular or a touch-tone telephone, a web-browser or email client in its readily available, out-of-box configuration is able to transmit short messages (up to a few hundred bits), performing complex calculations involving strong asymmetric cryptography requires additional tools which not everyone possesses or can afford to run. The fact that it is impossible to transact without performing complex calculations in real time is a far more serious obstacle than the need to contact the issuer for each transaction.

This is an interesting approach, but I suspect may be correct only in the limited sense that these devices and software don't come built-in with the particular cryptographic protocols needed for strongly private cash (e.g. Chaumian blinding). But they don't come built-in with digital cash software either. Thus, the main advantage of Nagy's scheme, which may or may not make up for its reduced privacy features, comes from the ability to use it without having to install any extra software at all -- to just, for example, cut and paste the cash from an e-mail where you received it from one person to an e-mail where you pay it to another. Your word processor can be your wallet. If this is an important use-case, then Nagian cash may succeed where Chaumian cash failed.

Another payment system of note is WebMoney, which recently started up a gold-backed currency, a competitor to the troubled e-gold. (HT: Financial Cryptography)

Posted by Nick Szabo at 1:15 PM

12 comments:

Mark Herpel said...

The new Webmoney Gold Purse is fantastic. The WMG system is an easy way to do commercial business around the globe. Since they have already partnered with Ukash, paysafecard and cashU its a snap to locally fund the WMG account with cash in most countries now and Webmoney is being accepted more and more in large markets like China. Not to mention their 'cash-in' kiosks in and around Russia where you can walk up and stick cash into the kiosk and instantly fund your WM account, now that is amazing.

Mark

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ▼ 2007 (47)
  - ► December (1)
  - ► October (2)
  - ► September (8)
  - ▼ August (10)
    - Money and the problem of cooperation
    - Why the industrial revolution?
    - Mutually private computation
    - Blind signatures
    - Personal jurisdiction before sovereignty
    - Smart contracts watch
    - Exit and freedom
    - Our new omniscient savior
    - Ten ways to make a political difference
    - Government for profit
  - ► July (4)
  - ► June (4)
  - ► May (8)
  - ► April (1)
  - ► March (2)
  - ► February (4)
  - ► January (3)

DigitalMoneyWorld

5:46 AM

► 2006 (130)
► 2005 (44)

nick said...

All interesting, but WMG suffers from the same basic vulnerability as e-gold and similar systems, as amply demonstrated by the recent e-gold woes. What legal and security protections is does WMG have in place to avoid a repeat of the forfeitures suffered by e-gold and its customers, and as suffered by holders of gold throughout history?

1:46 PM

Daniel A. Nagy said...

This comment has been removed by the author.

2:56 PM

Daniel A. Nagy said...

Now, it's my turn to perform a small jig for getting a mention at Unenumerated.

Now, back to business: asymmetric cryptography on-the-go is still expensive. On the simplest programmable mobile phones of which there are millions, an asymmetric primitive such as taking powers modulo large numbers takes about a minute. On high-end phones, it's around 500 milliseconds, which is still not quite "instantaneous", though already within the realm of acceptability. The reason is that the mobile industry "use their Moore's Law bounty to buy battery life", as Ian Grigg deftly puts it.

Another big challenge in digital payment in particular and smart contracts in general (I believe payment to be a special case of smart contracts in the emerging science of cyberlaw) is arbitration. It should be cheap, fast and universally available. This requires quite a bit of infrastructural investment and automation of things hitherto done "by hand" (using very expensive TTPs). Sure, the best smart contracts are self-enforcing, but disputes are unavoidable.

Two existing technologies have enormous potential for cyberlaw (or robot law, as Nick calls it):

1. OpenPGP. One of the features of OpenPGP that is not used to its full potential is the fact that owners of keys can make public statements about one another, assessing each-other's trustworthiness or, more generally, it is possible to establish and track reputation.

Once a key with its signatures is uploaded to the PKS network (a network of "gossiping" servers that eventually spread such information to all the others), it is irreversibly published. It can be revoked, but it cannot be erased.

Of course, there is the problem of libel, but I believe that it can be dealt with is several ways.

2. Git. A content-addressed repository for tracking changes and developments in a body of textual documents, originally conceived for the software source code.

However, it just happens to be the perfect medium for storing and developing cyberlaw.

P.S. The theory outlined in that 2005 paper of mine is slowly but surely developing into something hopefully practical. One of the more interesting things that we are about to start implementing is the so-called "conditional draft"; a reasonably general form of smart contract, with very diverse uses. Many financial instruments can be conveniently implemented using this abstraction.

3:07 PM

nick said...

DN: "On high-end phones, it's around 500 milliseconds, which is still not quite "instantaneous", though already within the realm of acceptability. The reason is that the mobile industry "use their Moore's Law bounty to buy battery life", as Ian Grigg deftly puts it."

That's an important point, but do these numbers take into account crypto in advanced mathematical algebras like elliptic curve, NTRU, etc? There can be an orders-of-magnitude speedup. Google tunrs up a number of blind signatures implemented in elliptic curves, for example this one.

Algebras like elliptic curve allow shorter keys and/or less CPU-intensive crypto operations for the same strength than RSA and normal discrete-log based crypto. ECC was being used for cell phones ten years ago. There have been a variety of new algebras (fields, rings, etc.) used for crypto since Chaum invented blinding, and I would imagine (though I must admit the math is beyond me) that blinding can be made to work in most of them if not all. (I'm pretty confident that blinding can be made to work in any analogs of RSA or DSA, e.g. the elliptic curve analog of DSA as in the above-linked paper). Of course, some of these may still be patent burdened. (Although basic ECC and Chaum's blind signatures are both off-patent, and combinations of blind signatures with other mathematical fields seem obvious to me, especially where they are just analogs of RSA or DSA, but that is certainly not a legal opinion :-)

4:18 PM

nick said...

DN: "Sure, the best smart contracts are self-enforcing, but disputes are unavoidable."

Given the extremely high costs, when compared to computer operations, of both human dispute resolution in particlar and trusted third parties in security protocols generally, the best way to deal with disputes will often be what in law we call "the common law rule of tough": on occasion the outcome of applying the rules to the facts will be unfair, and that's just tough luck. Sometimes there is a bug and and somebody has to absorb the costs. That's the philosophy of both common law and software protocols.

The competing philosophy, equity, tries to resolve each and every dispute fairly. If the rules applied to the facts are not fair, the judge simply decides what seems fair to him. This is a very expensive proposition in law. Giving judges this discretion leads to uncertainty and arbitrariness at least as often as it leads to greater fairness. Equity is, perhaps thankfully, quite unavailable for smart contracts, unless we count random number generators. :-)

Because they are computer protocols, the numbers of orders of magnitude efficiency gain turning, where possible, contractual terms into self-enforcing smart contracts -- even at the cost of occasional injustice -- is quite large. And a wide variety of new kinds of contracts, such as many new consumer derivatives and nanobarter, are made possible that are quite infeasible with just paper or mere signed text.

Of course, as yet only a tiny fraction of legal rules and contractual terms can be translated into software, and then often only in a highly abstracted manner. When the smart contract by itself produces enough unfairness, one can still use smart contracts to shift the burden of lawsuit, in the same way that repo men shift the burden of who has to sue over possession of a car.

4:46 PM

Daniel A. Nagy said...

The numbers that I give are for RSA. The problem with *all* the other blinding schemes is that they require (at least) an extra round of communication, which is very expensive in a mobile environment at the moment (the only exception being WiFi, but that is not universally available and has its own set of problems), and slow.

ECC-based asymmetric crypto is approximately 10 times faster than comparable traditional RSA or DH. But all practical ECC schemes are DH-replacements, not RSA.

An interesting contender is multi-prime RSA, which is about 2 to 3 times slower than ECC, but still much faster than traditional RSA. Chaumian blinding works perfectly with this one.

Actually, the fastest and simplest asymmetric crypto primitive is also an RSA-derivative, with correctly chosen paramenters. However, I am not aware of any signature schemes based on it (I tried to come up with one myself, but no success so far), let alone blinded ones.

Paranoid RSA, if used for better performance rather than increased security (the original linked paper does the latter, but it is trivial to rework it for our purpose) is twice as fast as comparable ECC, but it can only be used for decryption and identification (which I didn't manage to turn into a signature scheme).

NTRU is an interesting option, but I know too little about it to make confident statements.

2:33 PM

Daniel A. Nagy said...

WebMoney has a more sound governance model than e-gold. There is a clear separation of roles: underwriter and payment system operator. Which makes the TTP far more trustworthy. For their most successful issues (USD and Gold based, called WMZ and WMG, respectively), they actually walked the extra mile of placing the two TPs in different jurisdictions.

2:39 PM

nick said...

Daniel, that's very interesting and informative crypto stuff, thanks. If you want to write up a small article the topic of advanced blind signatures, and if you can think of a simplified description of your own scheme, I'd be happy to have you guest-post on the subject.

DN: "The problem with all the other blinding schemes is that they require (at least) an extra round of communication."

I didn't know this, and I agree it is pretty expensive.

I think we should also look at the attack model. It doesn't pay for the attacker to spend more than a dollar of CPU time to break the signature on a dollar "coin." The typical crypto key size requires far more than trillions of dollars worth of CPU cycles to crack. Although one must handle the risk of cracking algorithmic improvvements -- but there are ways to do this besides key size overkill -- I think the key sizes can be much smaller for low-denomination coins.

In comparison to another privacy model that is less than fully strong crypto, the appropriate blinding operation can also can have a small key size, although I don't know if that is significant in the scheme of things.

DN: "[WebMoney] actually walked the extra mile of placing the two TPs in different jurisdictions."

This is a good idea, assuming the jurisdictions are sufficiently independent. I'm not convinced it's sufficient to protect against what happened to e-gold, or against various similar threats, but it does seem to be a significcant improvement.

3:02 PM

Daniel A. Nagy said...

For dollar-denominated issue the two jurisdictions are Moscow, RF and Delaware, USA.
For gold, it's Moscow, RF and Dubai, UAE.

3:36 AM

Iang said...

What happened to e-gold would take a book to discuss!

In essence, and following my opinion only (a) they implemented parts of the five parties model, but not all, (b) they stayed in the US, knowing that the US was disinclined towards their business, and (c) the five parties model is more a model of governance than external security.

The five parties model postulates that the issuer should have no direct power over the asset, because any such power will lead to abuse. Instead, a technical operator (like a gold vault) would deal with a signatory that would initiate the actions, following a script. The other two parties are the day-to-day manager, and the public who are charged with continuous supervision.

e-gold implemented this model for gold bricks, but not for the digital side. AFAIR, goldmoney and Pecunix both completed the full model for both gold and digital gold.

It is certainly pleasing to see that WebMoney have implemented some elements of the five parties model, at least.

The question of putting those elements across different jurisdictions is complicated. For example, e-gold had their gold outside the US, but the US successfully seized some parts of it. If we look at the WebMoney situation, I'd say it is no stretch of the imagination to consider a Gazprom scenario.

For this reason, the most important factor is the fifth party: the public needs to make their own choices, and for that they need the full and continuous disclosure of what exactly the governance equation is.

e-gold fell far short in dealing with the fifth party, and I would suggest that any element of failure of disclosure should be seen as a sign that not all is well. The basic guideline is that if you are not governed by the government, and you are not governed by the public, then you are ungoverned. Self-governance doesn't work for serious amounts of money.

10:29 AM

nick said...

Ian: great comments, thanks!

4:37 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.